y-COORDINATES OF ELLIPTIC CURVES

JA KYUNG KOO AND DONG HWA SHIN

Abstract. By a change of variables we obtain new y-coordinates of elliptic curves. Utilizing these y-coordinates as modular functions, together together with the elliptic modular function, we generate the modular function fields of level N (≥ 3) (Theorems 3.11 and 3.13). Furthermore, by means of the singular values of the y-coordinates we construct the ray class fields modulo N over imaginary quadratic fields (Theorem 5.4) as well as normal bases of these ray class fields (Theorem 6.2).

1. Introduction

The Kronecker-Weber theorem asserts that any finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field $\mathbb{Q}(e^{2\pi i/n})$ for a positive integer n, whose significance is that it shows how to generate abelian extensions of $\mathbb{Q}$ via an analytic function $e^{2\pi iz}$ when evaluated at a rational number $1/n$. After this theorem Hilbert proposed at the Paris ICM in 1900 his 12^{th} problem which reads

> "it may be possible to find, for an arbitrary number field K, a transcendental function whose value generates a class field of K."

As for abelian extensions of an imaginary quadratic field, it was classically accomplished with modular functions from the theory of complex multiplication. Namely, the modular functions play a role analogous to the exponential function as in the case of $\mathbb{Q}$. But there is certain weakness that it requires at least two values of modular functions, for example, those of the elliptic modular function and the Weber function, to generate a ray class field of an imaginary quadratic field ([6] or [11, Chapter 10 Corollary to Theorem 7]).

On the other hand, Ramachandra ([15, Theorem 10]) constructed in 1964 a primitive generator of any abelian extension over an imaginary quadratic field by using the Siegel-Ramachandra invariants. Although he completely settled down the Hilbert 12^{th} problem in the case of imaginary quadratic fields, his invariants involve too complicated products of high powers of singular values of the Klein forms and singular values of the discriminant function. Recently Cho and Koo ([1, Corollary 5.5]) also succeeded in obtaining a primitive generator from Hasse's two singular values of the elliptic modular function and the Weber function. To this end they first showed that the singular value of the Weber function is an algebraic integer and then adopted the result of Gross and Zagier ([5] or [2, Theorem 13.28]) about prime factors of differences of singular values of the elliptic modular function. However, those invariants do not seem to be practical in use, in other words, one can hardly compute the minimal polynomials from them.

The theory of complex multiplication is based on the arithmetic of an elliptic curve E corresponding to the ring of integers of an imaginary quadratic field K. Here, by an elliptic curve we usually mean a smooth curve of genus one as a Lie group which can be viewed as the locus of a

2000 *Mathematics Subject Classification.* 11F11, 11G15, 11R37.

Key words and phrases. Elliptic curves, modular forms and functions, ray class fields, Siegel functions.

This research was supported by Basic Science Research Program through the NRF of Korea funded by MEST (2010-0001654). The second named author is partially supported by TJ Park Postdoctoral Fellowship.

Weierstrass equation of two affine variables x and y. In this paper we focus on the y-coordinates of the Weierstrass model of E to generate the modular function fields of level N (≥ 3) (Theorems 3.11 and 3.13). And, we further construct primitive generators of the ray class fields $K_{(N)}$ modulo N over K in terms of the singular values of those y-coordinates (Theorem 5.4) unlike the classical case ([6]) where the x-coordinates contribute in this matter instead. As its application we find a normal basis of $K_{(N)}$ (Theorem 6.2). We hope that this work will not only enrich the classical theory of complex multiplication, but also make us recognize the power of Shimura's reciprocity law.

2. Modular curves and modular forms

We shall first briefly review from [3, Chapter 2] the modular curve of level N and modular forms.

Let $\mathfrak{H} = \{\tau \in \mathbb{C}; \mathrm{Im}(\tau) > 0\}$ be the complex upper half-plane which inherits the Euclidean topology as a subspace of $\mathbb{R}^2$. The modular group

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix};\ a, b, c, d \in \mathbb{Z} \text{ such that } ad - bc = 1 \right\}$$

acts on $\mathfrak{H}$ by fractional linear transformations

$$\begin{array}{rrcl} \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ : & \mathfrak{H} & \longrightarrow & \mathfrak{H} \\ & \tau & \mapsto & \gamma(\tau) = (a\tau + b)/(c\tau + d). \end{array}$$

Then two elements of $\mathrm{SL}_2(\mathbb{Z})$ give rise to the same action on $\mathfrak{H}$ if and only if they differ by $\pm 1_2 = \pm\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

For a positive integer N let $\Gamma = \Gamma(N)$ be the principal congruence subgroup of level N, namely,

$$\Gamma = \Gamma(N) = \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z})\ ;\ \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

The natural projection

$$\pi\ :\ \mathfrak{H} \longrightarrow Y(N) = \Gamma\backslash\mathfrak{H} = \{\Gamma\tau\ ;\ \tau \in \mathfrak{H}\}$$

gives $Y(N)$ the quotient topology so that π is an open mapping. For each point $z \in \mathfrak{H}$, if

$$\Gamma_z = \{\gamma \in \Gamma\ ;\ \gamma(z) = z\}$$

denotes the isotropy subgroup of z which is finite cyclic, then there exists a neighborhood U_z of z in $\mathfrak{H}$ such that the set $\{\gamma \in \Gamma; \gamma(U_z) \cap U_z \neq \emptyset\}$ is exactly Γ_z. Now we define a map

$$\begin{array}{rcl} \psi_z\ :\ U_z & \longrightarrow & \mathbb{C} \\ \tau & \mapsto & ((\tau - z)/(\tau - \overline{z}))^{|\pm\Gamma_z/\{\pm 1_2\}|}. \end{array}$$

Its image $V_z = \psi_z(U_z)$ is an open subset of $\mathbb{C}$ by the open mapping theorem, and there exists a natural injection $\varphi_z : \pi(U_z) \to V_z$ such that $\psi_z = \varphi_z \circ \pi$. The map φ_z becomes the local coordinate, that is, the coordinate neighborhood about $\pi(z)$ in $Y(N)$ is $\pi(U_z)$ and the map $\varphi_z : \pi(U_z) \to V_z$ is a homeomorphism. Since the transition maps between these coordinate charts are holomorphic, $Y(N)$ can be viewed as a Riemann surface, which is called the *modular curve of level* N.

To compactify the modular curve $Y(N)$ we consider the extended upper half-plane

$$\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{Q} \cup \{\infty\},$$

where the points in $\mathbb{Q} \cup \{\infty\}$ are called the *cusps*. The modular group $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathfrak{H}^*$ also by fractional linear transformations. For any $M > 0$ let

$$\mathcal{N}_M = \{\tau \in \mathfrak{H}\ ;\ \mathrm{Im}(\tau) > M\}.$$

Adjoin the sets

$$\gamma(\mathcal{N}_M \cup \{\infty\}) \quad \text{for all } M > 0 \text{ and } \gamma \in \mathrm{SL}_2(\mathbb{Z})$$

to the usual open sets of $\mathfrak{H}$ to serve as a basis of neighborhoods of the cusps, and take the resulting topology on $\mathfrak{H}^*$. Now consider the extended quotient

$$X(N) = \Gamma\backslash\mathfrak{H}^* = Y(N) \cup \Gamma\backslash(\mathbb{Q} \cup \{\infty\}),$$

which is Hausdorff, connected and compact. Give $X(N)$ the quotient topology and extend the natural projection to $\pi : \mathfrak{H}^* \to X(N)$. To make $X(N)$ a compact Riemann surface we have to give it complex charts. For $z \in \mathfrak{H}$ we just retain the complex chart $\varphi_z : \pi(U_z) \to V_z$. For a cusp $s \in \mathbb{Q} \cup \{\infty\}$ take a matrix $\gamma_s \in \mathrm{SL}_2(\mathbb{Z})$ which maps s to ∞, and define a map

$$\begin{array}{rcccl} \psi_s & : & U_s = \gamma_s^{-1}(\mathcal{N}_2 \cup \{\infty\}) & \longrightarrow & \mathbb{C} \\ & & \tau & \mapsto & e^{2\pi i \gamma_s(\tau)/|\mathrm{SL}_2(\mathbb{Z})_\infty/\pm\Gamma_\infty|}. \end{array}$$

If $V_s = \psi_s(U_s)$ is its image which is an open subset of $\mathbb{C}$, then there exists a natural bijection $\varphi_s : \pi(U_s) \to V_s$ such that $\varphi_s \circ \pi = \psi_s$. It is routine to check that φ_s is a homeomorphism and the transition maps between charts of $X(N)$ are holomorphic. Therefore the extended quotient $X(N)$ is now a compact Riemann surface and also called the *modular curve of level* N.

For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and an integer k we define the *weight-k slash operator* $\cdot|[\gamma]_k$ on functions $f : \mathfrak{H} \to \widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ to be

$$(f|[\gamma]_k)(\tau) = (c\tau + d)^{-k} f(\gamma(\tau)) \quad (\tau \in \mathfrak{H}).$$

Definition 2.1. Let N (≥ 1) and k be integers. A function $f : \mathfrak{H} \to \widehat{\mathbb{C}}$ is a *modular form of level N and weight k* if

(i) f is meromorphic on $\mathfrak{H}$,
(ii) f invariant under $\cdot|[\gamma]_k$ for all $\gamma \in \Gamma(N)$,
(iii) $f|[\gamma]_k$ is meromorphic at ∞ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

To discuss meromorphy of f at ∞ we note that $\left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$ and f has period N. Hence f can be written as a Laurent series on some punctured disc about 0 with respect to $e^{2\pi i\tau/N}$. Let

$$q_\tau = e^{2\pi i \tau} \quad (\tau \in \mathfrak{H}).$$

If the Laurent series with respect to $q_\tau^{1/N}$ truncates from the left, that is, if

$$f = \sum_{n \geq m}^{\infty} c_n q_\tau^{n/N} \quad (c_n \in \mathbb{C})$$

for some integer m, then f is said to be *meromorphic at* ∞. The series is conventionally called the *Fourier expansion of* f.

Modular forms of level N and weight 0 are called *modular functions of level* N. They are exactly meromorphic functions defined on the modular curve $X(N)$ and vice versa. We denote the field of all modular functions of level N by $\mathbb{C}(X(N))$.

3. Elliptic curves and modular functions

In this section we shall explain modular function fields in terms of y-coordinates of elliptic curves together with the elliptic modular function.

An *elliptic curve* is a pair (E, O), where E is a smooth projective curve of genus one and $O \in E$. By the Riemann-Roch theorem every elliptic curve defined over $\mathbb{C}$ can be represented by the Weierstrass equation of the form

$$y^2 = 4x^3 - g_2 x - g_3 \quad \text{for some } g_2,\ g_3 \in \mathbb{C} \text{ such that } g_2^3 - 27g_3^2 \neq 0$$

with $O = [0 : 1 : 0]$ in the projective plane $\mathbb{P}^2(\mathbb{C})$ with homogeneous coordinates $[X : Y : Z]$, and vice versa ([18, Chapter III §1]).

Let Λ be a lattice in $\mathbb{C}$. If $\{\omega_1, \omega_2\}$ is a basis of Λ over $\mathbb{Z}$, then we write $\Lambda = [\omega_1, \omega_2]$. Unless otherwise specified we always assume that ω_1/ω_2 lies in $\mathfrak{H}$. A meromorphic function $f : \mathbb{C} \to \widehat{\mathbb{C}}$ is called an *elliptic function relative to* Λ if it is Λ-periodic, that is,

$$f(z + \omega) = f(z) \quad \text{for all } z \in \mathbb{C} \text{ and } \omega \in \Lambda.$$

Define the *Weierstrass $\wp$-function* (relative to Λ) as

$$\wp(z; \Lambda) = 1/z^2 + \sum_{\omega \in \Lambda - \{0\}} (1/(z - \omega)^2 - 1/\omega^2) \quad (z \in \mathbb{C}). \tag{3.1}$$

Since the above summation converges absolutely, we see that $\wp(z; \Lambda)$ is an even elliptic function relative to Λ with derivative

$$\wp'(z; \Lambda) = (d/dz)\wp(z; \Lambda) = -2 \sum_{\omega \in \Lambda} 1/(z - \omega)^3.$$

It is well-known that $\wp(z; \Lambda)$ and $\wp'(z; \Lambda)$ generate the field of all elliptic functions relative to Λ ([18, Chapter VI Theorem 3.2]).

Define the constants (relative to Λ)

$$g_2(\Lambda) = 60 \sum_{\omega \in \Lambda - \{0\}} 1/\omega^4, \quad g_3(\Lambda) = 140 \sum_{\omega \in \Lambda - \{0\}} 1/\omega^6 \quad \text{and} \quad \Delta(\Lambda) = g_2(\Lambda)^3 - 27g_3(\Lambda)^2. \tag{3.2}$$

The fact $\Delta(\Lambda) \neq 0$ implies that the curve given by

$$y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$$

is smooth so it gives rise to an elliptic curve E over $\mathbb{C}$. And, the map

$$\begin{array}{rcl} \varphi \ : \ \mathbb{C}/\Lambda & \longrightarrow & E(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C}) \\ z \pmod{\Lambda} & \mapsto & \begin{cases} [\wp(z; \Lambda) : \wp'(z; \Lambda) : 1] & \text{if } z \notin \Lambda \\ [0 : 1 : 0] & \text{if } z \in \Lambda \end{cases} \end{array}$$

becomes a complex analytic isomorphism of complex Lie groups, that is, an isomorphism of Riemann surfaces which is also a group homomorphism ([18, Chapter VI Proposition 3.6(b)]). Here, $\mathbb{C}/\Lambda$ has natural structure of a Riemann surface induced from that of $\mathbb{C}$, and has the group structure from the addition of complex numbers. Also $E(\mathbb{C})$ is a Riemann surface as a smooth curve which can be given a group structure by using some geometry ([18, Chapter III Theorem 3.6]).

Define the *j-invariant* $j(\Lambda)$ of the lattice Λ as

$$j(\Lambda) = 1728 g_2(\Lambda)^3/\Delta(\Lambda) = 1728 g_2(\Lambda)^3/(g_2(\Lambda)^3 - 27g_3(\Lambda)^2). \tag{3.3}$$

Now we define the *elliptic modular function* $j(\tau)$ as

$$j(\tau) = j([\tau, 1]) \quad (\tau \in \mathfrak{H}),$$

and

$$g_2(\tau) = g_2([\tau, 1]), \quad g_3(\tau) = g_3([\tau, 1]) \quad \text{and} \quad \Delta(\tau) = \Delta([\tau, 1]).$$

Proposition 3.1. *For $\tau \in \mathfrak{H}$ we have the following Fourier expansions*

$$\begin{aligned} g_2(\tau) &= ((2\pi)^4/12)(1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q_\tau^n), \\ g_3(\tau) &= ((2\pi)^6/216)(1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q_\tau^n), \\ \Delta(\tau) &= (2\pi i)^{12} q_\tau \prod_{n=1}^{\infty} (1 - q_\tau^n)^{24}, \end{aligned}$$

where $\sigma_k(n) = \sum_{d>0, d|n} d^k$.

Proof. See [11, Chapter 4 §1]. □

Together with the definition (3.2), the above proposition shows that $g_2(\tau)$, $g_3(\tau)$ and $\Delta(\tau)$ are modular forms of level 1 and weight 4, 6 and 12, respectively. Hence $j(\tau)$ is a modular function of level 1 with rational Fourier coefficients as follows:

$$\begin{aligned} j(\tau) &= 1/q_\tau + 744 + 196884 q_\tau + 21493760 q_\tau^2 + 864299970 q_\tau^3 + 20245856256 q_\tau^4 \\ &\quad + 333202640600 q_\tau^5 + 4252023300096 q_\tau^6 + 44656994071935 q_\tau^7 + 401490886656000 q_\tau^8 + \cdots . \end{aligned}$$

For an integer N (≥ 2) and a pair of rational numbers $(r_1, r_2) \in (1/N)\mathbb{Z}^2 - \mathbb{Z}^2$ we define a *Fricke function of level N* as

$$f_{(r_1,r_2)}(\tau) = -(2^7 3^5 g_2(\tau) g_3(\tau)/\Delta(\tau)) \wp(r_1\tau + r_2; [\tau, 1]) \quad (\tau \in \mathfrak{H}).$$

Note that $\wp(r_1\tau + r_2; [\tau, 1])$ is a modular form of level N and weight 2 by the definition (3.1) and has the expansion formula

$$\begin{aligned} &\wp(z; [\tau, 1]) = \wp(r_1\tau + r_2; [\tau, 1]) \qquad (3.4) \\ &= (2\pi i)^2 (1/12 + q_z/(1 - q_z)^2 + \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} n q_\tau^{mn} (q_z^n + q_z^{-n}) - 2 \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} n q_\tau^{mn}), \end{aligned}$$

where $q_z = e^{2\pi i z}$ ([11, Chapter 4 Proposition 2]). Hence $f_{(r_1,r_2)}(\tau)$ becomes a modular function of level N whose Fourier expansion with respect to $q_\tau^{1/N}$ has coefficients in $\mathbb{Q}(e^{2\pi i/N})$. Furthermore, it satisfies

$$\begin{aligned} &f_{(r_1,r_2)}(\tau) \circ \gamma = f_{(r_1,r_2)\gamma}(\tau) \quad \text{for any } \gamma \in \mathrm{SL}_2(\mathbb{Z}), \\ &f_{(r_1,r_2)}(\tau) = f_{(-r_1,-r_2)}(\tau) = f_{(r_1+a, r_2+b)}(\tau) \quad \text{for any } (a, b) \in \mathbb{Z}^2. \end{aligned}$$

Proposition 3.2. *We have $\mathbb{C}(X(1)) = \mathbb{C}(j(\tau))$. If $N \geq 2$, then*

$$\mathbb{C}(X(N)) = \mathbb{C}(j(\tau), f_{(r_1,r_2)}(\tau))_{(r_1,r_2)\in(1/N)\mathbb{Z}^2-\mathbb{Z}^2} = \mathbb{C}(j(\tau), f_{(1/N,0)}(\tau), f_{(1/N,0)}(\tau)).$$

Furthermore, $\mathbb{C}(X(N))$ is a Galois extension of $\mathbb{C}(X(1))$. Its Galois group is given by

$$\Gamma(1)/\pm\Gamma(N) \simeq \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\},$$

whose actions are fractional linear transformations.

Proof. See [11, Chapter 6 Theorems 1 and 2] and [3, Proposition 7.5.1]. □

For a positive integer N let $\zeta_N = e^{2\pi i/N}$. We denote

$$\mathcal{F}_N = \begin{cases} \mathbb{Q}(j(\tau)) & \text{if } N = 1 \\ \mathbb{Q}(j(\tau),\ f_{(r_1,r_2)}(\tau))_{(r_1,r_2)\in(1/N)\mathbb{Z}^2-\mathbb{Z}^2} & \text{if } N \geq 2, \end{cases}$$

and call it the *modular function field of level N over $\mathbb{Q}$*.

Proposition 3.3. *Let N be a positive integer. Then $\mathcal{F}_N$ coincides with the field of functions in $\mathbb{C}(X(N))$ whose Fourier expansions with respect to $q_\tau^{1/N}$ have coefficients in $\mathbb{Q}(\zeta_N)$. Furthermore, $\mathcal{F}_N$ is a Galois extension of $\mathcal{F}_1$ whose Galois group is represented by*

$$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\} = G_N \cdot \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\} = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\} \cdot G_N,$$

where

$$G_N = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \ ;\ d \in (\mathbb{Z}/N\mathbb{Z})^* \right\}.$$

First, the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) \in G_N$ acts on $\sum_{n\geq m}^\infty c_n q_\tau^{n/N} \in \mathcal{F}_N$ by

$$\sum_{n\geq m}^{\infty} c_n q_\tau^{n/N} \mapsto \sum_{n\geq m}^{\infty} c_n^{\sigma_d} q_\tau^{n/N},$$

where σ_d is the automorphism of $\mathbb{Q}(\zeta_N)$ induced by $\zeta_N \mapsto \zeta_N^d$. And, for an element $\gamma \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}$ let $\gamma' \in \mathrm{SL}_2(\mathbb{Z})$ be a preimage of γ via the natural surjection $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}$. Then γ acts on $h \in \mathcal{F}_N$ by composition

$$h \mapsto h \circ \gamma'.$$

Proof. See [17, Proposition 6.9(1)] and [11, Chapter 6 Theorem 3]. □

For a lattice Λ in $\mathbb{C}$ the *Weierstrass σ-function* (relative to Λ) is defined by

$$\sigma(z;\Lambda) = z \prod_{\omega\in\Lambda-\{0\}} (1 - z/\omega) e^{z/\omega + (1/2)(z/\omega)^2} \quad (z \in \mathbb{C}).$$

Taking the logarithmic derivative we define the *Weierstrass ζ-function* (relative to Λ)

$$\zeta(z;\Lambda) = \sigma'(z;\Lambda)/\sigma(z;\Lambda) = 1/z + \sum_{\omega\in\Lambda-\{0\}} (1/(z-\omega) + 1/\omega + z/\omega^2) \quad (z \in \mathbb{C}).$$

Differentiating the function $\zeta(z+\omega;\Lambda) - \zeta(z;\Lambda)$ for any $\omega \in \Lambda$ results in 0, because $\zeta'(z;\Lambda) = -\wp(z;\Lambda)$ and $\wp(z;\Lambda)$ is periodic with respect to Λ. Hence there is a constant $\eta(\omega;\Lambda)$ such that

$$\zeta(z+\omega;\Lambda) = \zeta(z;\Lambda) + \eta(\omega;\Lambda).$$

For $(r_1, r_2) \in \mathbb{Q}^2 - \mathbb{Z}^2$ we define the *Klein form* $\mathfrak{k}_{(r_1,r_2)}(\tau)$ as

$$\mathfrak{k}_{(r_1,r_2)}(\tau) = e^{-\frac{1}{2}(r_1\eta(\tau;[\tau,1]) + r_2\eta(1;[\tau,1]))(r_1\tau + r_2)} \sigma(r_1\tau + r_2; [\tau, 1]) \quad (\tau \in \mathfrak{H}). \tag{3.5}$$

Proposition 3.4. (i) *For $(r_1, r_2) \in \mathbb{Q}^2 - \mathbb{Z}^2$ we have*

$$\mathfrak{k}_{(-r_1,-r_2)}(\tau) = -\mathfrak{k}_{(r_1,r_2)}(\tau).$$

(ii) *For $(r_1, r_2) \in \mathbb{Q}^2 - \mathbb{Z}^2$ and $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ we get*

$$\mathfrak{k}_{(r_1,r_2)}(\tau) \circ \gamma = (c\tau + d)^{-1} \mathfrak{k}_{(r_1,r_2)\gamma}(\tau).$$

(iii) *For* $(r_1, r_2) \in \mathbb{Q}^2 - \mathbb{Z}^2$ *and* $(s_1, s_2) \in \mathbb{Z}^2$ *we get*

$$\mathfrak{k}_{(r_1+s_1, r_2+s_2)}(\tau) = \varepsilon((r_1, r_2), (s_1, s_2))\mathfrak{k}_{(r_1,r_2)}(\tau),$$

where $\varepsilon((r_1, r_2), (s_1, s_2)) = (-1)^{s_1 s_2 + s_1 + s_2} e^{-\pi i(s_1 r_2 - s_2 r_1)}$.

Proof. See [10, pp.27–28]. □

Now we define the *Siegel function* $g_{(r_1,r_2)}(\tau)$ for $(r_1, r_2) \in \mathbb{Q}^2 - \mathbb{Z}^2$ as

$$g_{(r_1,r_2)}(\tau) = \mathfrak{k}_{(r_1,r_2)}(\tau)\eta^2(\tau) \quad (\tau \in \mathfrak{H}). \tag{3.6}$$

Here, $\eta(\tau)$ is the *Dedekind* η*-function* defined by

$$\eta(\tau) = \sqrt{2\pi}\zeta_8 q_\tau^{1/24} \prod_{n=1}^{\infty}(1 - q_\tau^n) \quad (\tau \in \mathfrak{H}), \tag{3.7}$$

which satisfies

$$\eta^2(\tau) \circ S = \zeta_{12}^9 \tau \eta^2(\tau), \tag{3.8}$$
$$\eta^2(\tau) \circ T = \zeta_{12}\eta^2(\tau), \tag{3.9}$$

for $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ ([11, Chapter 18 Theorem 6]). We have the transformation formulas of Siegel functions as follows:

Proposition 3.5. (i) *For* $(r_1, r_2) \in \mathbb{Q}^2 - \mathbb{Z}^2$ *we have*

$$g_{(-r_1,-r_2)}(\tau) = -g_{(r_1,r_2)}(\tau).$$

(ii) *For* $(r_1, r_2) \in \mathbb{Q}^2 - \mathbb{Z}^2$ *we get*

$$\begin{aligned} g_{(r_1,r_2)}(\tau) \circ S &= \zeta_{12}^9 g_{(r_1,r_2)S}(\tau) &= \zeta_{12}^9 g_{(r_2,-r_1)}(\tau), \\ g_{(r_1,r_2)}(\tau) \circ T &= \zeta_{12} g_{(r_1,r_2)T}(\tau) &= \zeta_{12} g_{(r_1,r_1+r_2)}(\tau). \end{aligned}$$

(iii) *For* $(r_1, r_2) \in \mathbb{Q}^2 - \mathbb{Z}^2$ *and* $(s_1, s_2) \in \mathbb{Z}^2$ *we have*

$$g_{(r_1+s_1,r_2+s_2)}(\tau) = \varepsilon((r_1, r_2), (s_1, s_2))g_{(r_1,r_2)}(\tau),$$

where $\varepsilon((r_1, r_2), (s_1, s_2))$ *is the root of unity given in Proposition 3.4(iii).*

Proof. One can readily verify the formulas by using Proposition 3.4, (3.8) and (3.9). □

A Siegel function has a fairly simple order formula. Let $\mathbf{B}_2(X) = X^2 - X + 1/6$ be the second Bernoulli polynomial. Using the product formula of the Weierstrass σ-function

$$\sigma(z; [\tau, 1]) = (1/2\pi i)e^{(1/2)\eta(1;[\tau,1])z^2}(q_z^{1/2} - q_z^{-1/2}) \prod_{n=1}^{\infty}(1 - q_\tau^n q_z)(1 - q_\tau^n q_z^{-1})(1 - q_\tau^n)^{-2} \quad (\tau \in \mathfrak{H})$$

([11, Chapter 18 Theorem 4]) we get the following infinite product expression

$$g_{(r_1,r_2)}(\tau) = -q_\tau^{(1/2)\mathbf{B}_2(r_1)} e^{\pi i r_2(r_1-1)}(1 - q_z) \prod_{n=1}^{\infty}(1 - q_\tau^n q_z)(1 - q_\tau^n q_z^{-1}), \tag{3.10}$$

where $z = r_1\tau + r_2$. By analyzing (3.10) we obtain

$$\mathrm{ord}_{q_\tau}(g_{(r_1,r_2)}(\tau)) = \frac{1}{2}\mathbf{B}_2(\langle r_1 \rangle), \tag{3.11}$$

where $\langle X \rangle$ is the fractional part of $X \in \mathbb{R}$ such that $0 \leq \langle X \rangle < 1$ ([10, Chapter 2 §1]).

For a given integer N (≥ 2) Kubert and Lang provided a (necessary and sufficient) condition for a product of Siegel functions to be in $\mathcal{F}_N$. We say that a family of integers $\{m(r)\}_{r=(r_1,r_2)\in(1/N)\mathbb{Z}^2-\mathbb{Z}^2}$ with $m(r)=0$ except finitely many r satisfies the *quadratic relation modulo* N if

$$\sum_r m(r)(Nr_1)^2 \equiv \sum_r m(r)(Nr_2)^2 \equiv 0 \pmod{\gcd(2,N)\cdot N},$$
$$\sum_r m(r)(Nr_1)(Nr_2) \equiv 0 \pmod{N}.$$

Proposition 3.6. *Let N (≥ 2) be an integer and $\{m(r)\}_{r\in(1/N)\mathbb{Z}^2-\mathbb{Z}^2}$ be a family of integers such that $m(r)=0$ except finitely many r. Then a product of Siegel functions*

$$\prod_{r\in(1/N)\mathbb{Z}^2-\mathbb{Z}^2} g_r^{m(r)}(\tau)$$

belongs to $\mathcal{F}_N$, if $\{m(r)\}_r$ satisfies the quadratic relation modulo N and 12 divides $\gcd(12,N)\cdot\sum_r m(r)$.

Proof. See [10, Chapter 3 Theorems 5.2 and 5.3]. □

In particular, $g_r(\tau)$ and $g_r^{12N}(\tau)$ lie in $\mathcal{F}_{12N^2}$ and $\mathcal{F}_N$ for any $r\in(1/N)\mathbb{Z}^2-\mathbb{Z}^2$, respectively.

Proposition 3.7. *Let $(r_1,r_2)\in(1/N)\mathbb{Z}^2-\mathbb{Z}^2$ for an integer N (≥ 2). Then both $g_r(\tau)$ and $N/g_r(\tau)$ are integral over $\mathbb{Z}[j(\tau)]$.*

Proof. See [9, §3]. □

Proposition 3.8. *Let $(r_1,r_2)\in(1/N)\mathbb{Z}^2-\mathbb{Z}^2$ for an integer N (≥ 2). Then $g_{(r_1,r_2)}^{12N/\gcd(6,N)}(\tau)\in\mathcal{F}_N$. If $\alpha\in\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1_2\}\simeq\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)$, then*

$$g_{(r_1,r_2)}^{12N/\gcd(6,N)}(\tau)^\alpha = g_{(r_1,r_2)\alpha}^{12N/\gcd(6,N)}(\tau).$$

Proof. By Proposition 3.6 we get the first assertion. The action of α is due to Propositions 3.3, 3.5 and the infinite product formula (3.10). □

Let Λ be a lattice in $\mathbb{C}$ of the form $\Lambda=[\tau,1]$ with $\tau\in\mathfrak{H}$. From the complex analytic isomorphism

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \stackrel{\sim}{\longrightarrow} & y^2=4x^3-g_2(\Lambda)x-g_3(\Lambda) \\ z & \mapsto & [\wp(z;\Lambda):\wp'(z;\Lambda):1], \end{array}$$

we have a relation

$$\wp'(z;\Lambda)^2 = 4\wp(z;\Lambda)^3 - g_2(\tau)\wp(z;\Lambda) - g_3(\tau).$$

Note that $\eta^{24}(\tau)=\Delta(\tau)=\Delta(\Lambda)$ $(\neq 0)$ by the definition (3.7) and Proposition 3.1. Diving both sides of the above equation by the nonzero constant $\eta^{12}(\tau)$ and using the relation

$$\wp'(z;\Lambda) = -\sigma(2z;\Lambda)/\sigma(z;\Lambda)^4$$

([18, p.166]) we get

$$\left(-\frac{\sigma(2z;\Lambda)\eta^2(\tau)}{\sigma(z;\Lambda)^4\eta^8(\tau)}\right)^2 = 4\left(\frac{\wp(z;\Lambda)}{\eta^4(\tau)}\right)^3 - \frac{g_2(\tau)}{\eta^8(\tau)}\frac{\wp(z;\Lambda)}{\eta^4(\tau)} - \frac{g_3(\tau)}{\eta^{12}(\tau)}.$$

Hence we obtain another isomorphism

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \stackrel{\sim}{\longrightarrow} & y^2=4x^3-(g_2(\tau)/\eta^8(\tau))x-g_3(\tau)/\eta^{12}(\tau) \\ z & \mapsto & [\wp(z;\Lambda)/\eta^4(\tau):\sigma(2z;\Lambda)\eta^2(\tau)/\sigma(z;\Lambda)^4\eta^8(\tau):1]. \end{array}$$

If $z = r_1\tau + r_2$ with $(r_1, r_2) \in \mathbb{Q}^2 - \mathbb{Z}^2$, then the corresponding y-coordinate satisfies

$$\sigma(2r_1\tau + 2r_2; \Lambda)\eta^2(\tau)/\sigma(r_1\tau + r_2; \Lambda)^4\eta^8(\tau) = g_{(2r_1,2r_2)}(\tau)/g^4_{(r_1,r_2)}(\tau) \tag{3.12}$$

by (3.5) and (3.6). Regarding τ as a variable on $\mathfrak{H}$ we define a function

$$y_{(r_1,r_2)}(\tau) = g_{(2r_1,2r_2)}(\tau)/g^4_{(r_1,r_2)}(\tau). \tag{3.13}$$

Lemma 3.9. *Let $(r_1, r_2) \in (1/N)\mathbb{Z}^2 - \mathbb{Z}^2$ for an integer N (≥ 2). Then $y^{4/\gcd(4,N)}_{(r_1,r_2)}(\tau) \in \mathcal{F}_N$.*

Proof. If $(2r_1, 2r_2) \in \mathbb{Z}^2$, then $y^{4/\gcd(4,N)}_{(r_1,r_2)}(\tau) = 0 \in \mathcal{F}_N$. So we assume $(2r_1, 2r_2) \notin \mathbb{Z}^2$. Now, the product of Siegel functions $(g_{(2r_1,2r_2)}(\tau)/g^4_{(r_1,r_2)}(\tau))^{4/\gcd(4,N)}$ satisfies the quadratic relation modulo N, and 12 divides

$$\gcd(12, N) \cdot \text{sum of exponents} = -12\gcd(12, N)/\gcd(4, N).$$

Thus the function belongs to $\mathcal{F}_N$ by Proposition 3.6. $\square$

Lemma 3.10. *Let N (≥ 3) and m $(\neq 0)$ be integers. If $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ acts trivially on $y^m_{(1/N,0)}(\tau)$ and $y^m_{(0,1/N)}(\tau)$ as a fractional linear transformation, then $\gamma \in \pm\Gamma(N)$.*

Proof. For convenience we use the notation $\doteq$ to denote the equality up to a root of unity. Letting $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ we derive by Proposition 3.5(ii) that

$$\begin{aligned} y^m_{(1/N,0)}(\tau)^\gamma &\doteq g^m_{(2/N,0)\gamma}(\tau)/g^{4m}_{(1/N,0)\gamma}(\tau) = g^m_{(2a/N,2b/N)}(\tau)/g^{4m}_{(a/N,b/N)}(\tau), \\ y^m_{(0,1/N)}(\tau)^\gamma &\doteq g^m_{(0,2/N)\gamma}(\tau)/g^{4m}_{(0,1/N)\gamma}(\tau) = g^m_{(2c/N,2d/N)}(\tau)/g^{4m}_{(c/N,d/N)}(\tau). \end{aligned}$$

Since we are assuming that the action of γ on $y^m_{(1/N,0)}(\tau)$ and $y^m_{(1/N,0)}(\tau)$ is trivial, we get

$$g^m_{(2a/N,2b/N)}(\tau)/g^{4m}_{(a/N,b/N)}(\tau) \doteq g^m_{(2/N,0)}(\tau)/g^{4m}_{(1/N,0)}(\tau), \tag{3.14}$$

$$g^m_{(2c/N,2d/N)}(\tau)/g^{4m}_{(c/N,d/N)}(\tau) \doteq g^m_{(0,2/N)}(\tau)/g^{4m}_{(0,1/N)}(\tau). \tag{3.15}$$

It then follows from the action of $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ on both side of (3.14) and (3.15) as a fractional linear transformation that

$$g^m_{(2b/N,-2a/N)}(\tau)/g^{4m}_{(b/N,-a/N)}(\tau) \doteq g^m_{(0,-2/N)}(\tau)/g^{4m}_{(0,-1/N)}(\tau), \tag{3.16}$$

$$g^m_{(2d/N,-2c/N)}(\tau)/g^{4m}_{(d/N,-c/N)}(\tau) \doteq g^m_{(2/N,0)}(\tau)/g^{4m}_{(1/N,0)}(\tau) \tag{3.17}$$

by Proposition 3.5(ii). Now by using the order formula (3.11) we can compare the orders of both sides of (3.14)$\sim$(3.17) with respect to q_τ to conclude

$$\begin{aligned} m(1/2)\mathbf{B}_2(\langle 2a/N\rangle) - 4m(1/2)\mathbf{B}_2(\langle a/N\rangle) &= m(1/2)\mathbf{B}_2(2/N) - 4m(1/2)\mathbf{B}_2(1/N), \\ m(1/2)\mathbf{B}_2(\langle 2c/N\rangle) - 4m(1/2)\mathbf{B}_2(\langle c/N\rangle) &= m(1/2)\mathbf{B}_2(0) - 4m(1/2)\mathbf{B}_2(0), \\ m(1/2)\mathbf{B}_2(\langle 2b/N\rangle) - 4m(1/2)\mathbf{B}_2(\langle b/N\rangle) &= m(1/2)\mathbf{B}_2(0) - 4m(1/2)\mathbf{B}_2(0), \\ m(1/2)\mathbf{B}_2(\langle 2d/N\rangle) - 4m(1/2)\mathbf{B}_2(\langle d/N\rangle) &= m(1/2)\mathbf{B}_2(2/N) - 4m(1/2)\mathbf{B}_2(1/N). \end{aligned}$$

Considering the fact $\det(\gamma) = ad - bc = 1$ we achieve $a \equiv d \equiv \pm 1 \pmod N$ and $b \equiv c \equiv 0 \pmod N$. Hence γ lies in $\pm\Gamma(N)$, as desired. $\square$

Theorem 3.11. *Let N (≥ 3) be an integer. For any nonzero integer m,*

$$\mathbb{C}(X(N)) = \mathbb{C}(j(\tau), y^{4m/\gcd(4,N)}_{(1/N,0)}(\tau), y^{4m/\gcd(4,N)}_{(0,1/N)}(\tau)).$$

Proof. By Proposition 3.2 we have
$$\mathrm{Gal}(X(N)/X(1)) \simeq \Gamma(1)/\pm\Gamma(N),$$
whose action is given by composition. Put
$$F = \mathbb{C}(j(\tau), y_{(1/N,0)}^{4m/\gcd(4,N)}(\tau), y_{(0,1/N)}^{4m/\gcd(4,N)}(\tau)),$$
which is a subfield of $\mathbb{C}(X(N))$ containing $\mathbb{C}(X(1)) = \mathbb{C}(j(\tau))$ by Lemma 3.9. Assume that an element $\gamma \in \Gamma(1)$ acts trivially on F. Then γ must be in $\pm\Gamma(N)$ by Lemma 3.10. Thus F is all of $\mathbb{C}(X(N))$ by Galois theory. □

Lemma 3.12. *Let N be a positive integer. If S is a subset of $\mathcal{F}_N$ such that $\mathbb{C}(X(N)) = \mathbb{C}(S)$, then $\mathcal{F}_N = \mathbb{Q}(\zeta_N, S)$.*

Proof. See [9, Lemma 4.1]. □

Theorem 3.13. *Let N (≥ 3) be an integer. For any nonzero integer m,*
$$\mathcal{F}_N = \mathbb{Q}(j(\tau), \zeta_N y_{(1/N,0)}^{4m/\gcd(4,N)}(\tau), y_{(0,1/N)}^{4m/\gcd(4,N)}(\tau)).$$

Proof. Set
$$F = \mathbb{Q}(j(\tau), \zeta_N y_{(1/N,0)}^{4m/\gcd(4,N)}(\tau), y_{(0,1/N)}^{4m/\gcd(4,N)}(\tau)),$$
which is a subfield of $\mathcal{F}_N$ containing $\mathcal{F}_1 = \mathbb{Q}(j(\tau))$ by Lemma 3.9. By Theorem 3.11 and Lemma 3.12 we have $\mathcal{F}_N = F(\zeta_N)$. Hence $\mathrm{Gal}(\mathcal{F}_N/F)$ is isomorphic to a subgroup of $G_N = \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) ; d \in (\mathbb{Z}/N\mathbb{Z})^*\}$ by Proposition 3.3. Assume that $\beta = \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) \in G_N$ acts trivially on F. Since
$$y_{(1/N,0)}(\tau) = \frac{-q_\tau^{(1/2)\mathbf{B}_2(2/N)}(1-q_\tau^{2/N})\prod_{n=1}^{\infty}(1-q_\tau^{n+2/N})(1-q_\tau^{n-2/N})}{(-q_\tau^{(1/2)\mathbf{B}_2(2/N)}(1-q_\tau^{2/N})\prod_{n=1}^{\infty}(1-q_\tau^{n+2/N})(1-q_\tau^{n-2/N}))^4}$$
has rational Fourier coefficients by (3.10), we get
$$\zeta_N y_{(1/N,0)}^{4m/\gcd(4,N)}(\tau) = (\zeta_N y_{(1/N,0)}^{4m/\gcd(4,N)}(\tau))^\beta = \zeta_N^d y_{(1/N,0)}^{4m/\gcd(4,N)}(\tau).$$
Therefore $d \equiv 1 \pmod{N}$, which implies that F is all of $\mathcal{F}_N$ by Galois theory. □

4. Shimura's reciprocity law

In this section we shall explicitly describe Shimura's reciprocity law due to Stevenhagen ([19, §3, 6]), from which we are able to precisely determine all the conjugates of the singular value of a modular function. To begin with we introduce some consequences of the main theorem of complex multiplication ([11, Chapter 10 Theorem 4]).

Let $\mathfrak{a}$ be a fractional ideal of an imaginary quadratic field K. From the uniformization
$$\begin{array}{rcccl} \varphi : \mathbb{C}/\Lambda & \xrightarrow{\sim} & E(\mathbb{C}) & : & y^2 = 4x^3 - g_2(\mathfrak{a})x - g_3(\mathfrak{a}) \\ z & \mapsto & [\wp(z;\mathfrak{a}) : \wp'(z;\mathfrak{a}) : 1], & & \end{array} \tag{4.1}$$
we define the *Weber function* h on $E(\mathbb{C})$ by
$$h([0:1:0]) = 0 \quad \text{and} \quad h(\varphi(z)) = \begin{cases} (g_2(\mathfrak{a})g_3(\mathfrak{a})/\Delta(\mathfrak{a}))\wp(z;\mathfrak{a}) & \text{if } j(\mathfrak{a}) \neq 0,\ 1728 \\ (g_2(\mathfrak{a})^2/\Delta(\mathfrak{a}))\wp(z;\mathfrak{a})^2 & \text{if } j(\mathfrak{a}) = 1728 \\ (g_3(\mathfrak{a})/\Delta(\mathfrak{a}))\wp(z;\mathfrak{a})^3 & \text{if } j(\mathfrak{a}) = 0 \end{cases} \quad \text{for } z \notin \mathfrak{a}. \tag{4.2}$$

Proposition 4.1. *Let K be an imaginary quadratic field and $\mathfrak{a}$ be a fractional ideal of K. Let N be any positive integer.*

(i) *If E is the elliptic curve given in (4.1) and h is the Weber function on $E(\mathbb{C})$ as in (4.2), then we have*
$$K_{(N)} = K(j(E), h(E[N])),$$
where $E[N]$ is the group of N-torsion points in $E(\mathbb{C})$ and $j(E) = j(\mathfrak{a})$. Moreover,
$$K_{(N)} = K(j(\mathfrak{a}), h(\varphi(\text{a generator of } (1/N)\mathfrak{a}/\mathfrak{a} \text{ as a module over } \mathcal{O}_K))).$$

(ii) *If $\mathfrak{a} = [z_1, z_2]$ with $z = z_1/z_2 \in \mathfrak{H}$, then we get*
$$K_{(N)} = K(f(z)\ ;\ f \in \mathcal{F}_N \text{ is finite and defined at } z).$$

Proof. See [11, Chapter 10 Theorems 2, 8 and their corollaries]. □

Let
$$\mathcal{F} = \bigcup_{N=1}^{\infty} \mathcal{F}_N$$
be the field of all modular functions over $\mathbb{Q}$. Passing to the projective limit of the exact sequences
$$1 \longrightarrow \{\pm 1_2\} \longrightarrow \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \longrightarrow \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1) \longrightarrow 1 \quad (N \geq 1),$$
which are obtained by Proposition 3.3, we derive an exact sequence
$$1 \longrightarrow \{\pm 1_2\} \longrightarrow \prod_{p\ :\ \text{primes}} \mathrm{GL}_2(\mathbb{Z}_p) \longrightarrow \mathrm{Gal}(\mathcal{F}/\mathcal{F}_1) \longrightarrow 1. \tag{4.3}$$
For every $u = (u_p)_p \in \prod_p \mathrm{GL}_2(\mathbb{Z}_p)$ and N (≥ 1), there exists an integral matrix α in $\mathrm{GL}_2^+(\mathbb{Q})$ such that $\alpha \equiv u_p \pmod{N\mathbb{Z}_p}$ for all p dividing N by the Chinese remainder theorem. Then the action of u on $\mathcal{F}_N$ is understood as the action of α ([17, Proposition 6.21]).

Let $\mathbb{A}_\mathbb{Q} = \prod_p' \mathbb{Q}_p$ denote the ring of finite adèles of $\mathbb{Q}$. Here, the restricted product is taken with respect to the subrings $\mathbb{Z}_p$ of $\mathbb{Q}_p$. Then every $x \in \mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$ can be written as
$$x = u \cdot \beta \text{ with } u \in \prod_p \mathrm{GL}_2(\mathbb{Z}_p) \text{ and } \beta \in \mathrm{GL}_2^+(\mathbb{Q})$$
([17, Lemma 6.19]). Such a decomposition determines a group action of $\mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$ on $\mathcal{F}$ by
$$h^x = h^u \circ \beta,$$
where h^u is given by the exact sequence (4.3) ([17, pp.149–150]). Then we have the following *Shimura's exact sequence*
$$1 \longrightarrow \mathbb{Q}^* \longrightarrow \mathrm{GL}_2(\mathbb{A}_\mathbb{Q}) \longrightarrow \mathrm{Aut}(\mathcal{F}) \longrightarrow 1$$
([17, Theorem 6.23]).

For an imaginary quadratic field K of discriminant d_K, we fix
$$\theta_K = \begin{cases} \sqrt{d_K}/2 & \text{for } d_K \equiv 0 \pmod 4 \\ (-1+\sqrt{d_K})/2 & \text{for } d_K \equiv 1 \pmod 4, \end{cases} \tag{4.4}$$
which belongs to $\mathfrak{H}$ and generates the ring of integers of K, namely, $\mathcal{O}_K = [\theta_K, 1]$. We use the notation $K_p = K \otimes_\mathbb{Q} \mathbb{Q}_p$ for each prime p and denote the group of finite idèles of K by $\mathbb{A}_K^* = \prod_p' K_p^*$, where the restricted product is taken with respect to the subgroups $\mathcal{O}_p^* = (\mathcal{O}_K \otimes_\mathbb{Z} \mathbb{Z}_p)^*$ of K_p^*. Let

K^{ab} stand for the maximal abelian extension of K and H be the Hilbert class field of K. Then the class field theory for K is summarized via the following exact sequence

$$1 \longrightarrow \mathcal{O}_K^* \longrightarrow \prod_p \mathcal{O}_p^* \xrightarrow{[\cdot,K]} \mathrm{Gal}(K^{\mathrm{ab}}/H) \longrightarrow 1, \tag{4.5}$$

where $[\cdot, K]$ is the Artin reciprocity map on K ([4, Chapter II §3 and 5]).

For each prime p we define a (regular) map

$$(g_{\theta_K})_p \ : \ K_p^* \longrightarrow \mathrm{GL}_2(\mathbb{Q}_p)$$

as an injection that sends $x_p \in K_p^*$ to the matrix in $\mathrm{GL}_2(\mathbb{Q}_p)$ which represents multiplication by x_p on K_p with respect to the $\mathbb{Q}_p$-basis $\begin{pmatrix}\theta_K\\ 1\end{pmatrix}$. More precisely, if we let B_{θ_K} and C_{θ_K} be integers such that

$$\min(\theta_K, \mathbb{Q}) = X^2 + B_{\theta_K}X + C_{\theta_K},$$

then we can describe the map as

$$(g_{\theta_K})_p \ : \ s_p\theta_K + t_p \mapsto \begin{pmatrix} t_p - B_{\theta_K}s_p & -C_{\theta_K}s_p \\ s_p & t_p \end{pmatrix} \quad ((s_p, t_p) \in \mathbb{Q}_p^2 - \{(0,0)\}).$$

On the idèle group $\mathbb{A}_K^*$ we achieve an injection

$$g_{\theta_K} = \prod_p (g_{\theta_K})_p \ : \ \mathbb{A}_K^* \longrightarrow {\prod_p}' \mathrm{GL}_2(\mathbb{Q}_p),$$

where the restricted product is taken with respect to the subgroups $\mathrm{GL}_2(\mathbb{Z}_p)$ of $\mathrm{GL}_2(\mathbb{Q}_p)$. Combining (4.3) and (4.5) we get the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{O}_K^* & \longrightarrow & \prod_p \mathcal{O}_p^* & \xrightarrow{[\cdot,K]} & \mathrm{Gal}(K^{\mathrm{ab}}/H) & \longrightarrow & 1 \\ & & & & \downarrow g_{\theta_K} & & & & \\ 1 & \longrightarrow & \{\pm 1_2\} & \longrightarrow & \prod_p \mathrm{GL}_2(\mathbb{Z}_p) & \longrightarrow & \mathrm{Gal}(\mathcal{F}/\mathcal{F}_1) & \longrightarrow & 1. \end{array} \tag{4.6}$$

Then *Shimura's reciprocity law* states that for $h \in \mathcal{F}$ and $x \in \prod_p \mathcal{O}_p^*$,

$$h(\theta_K)^{[x^{-1},K]} = h^{g_{\theta_K}(x)}(\theta_K) \tag{4.7}$$

([17, Theorem 6.31]).

Let $Q = [a, b, c] = aX^2 + bXY + cY^2 \in \mathbb{Z}[X, Y]$ be a primitive positive definite binary quadratic form of discriminant d_K. Under the properly equivalence relation these forms determine a finite abelian group $\mathrm{C}(d_K)$, called the *form class group of discriminant* d_K. In particular, the unit element is the class containing

$$\begin{cases} [1, 0, -d_K/4] & \text{for } d_K \equiv 0 \pmod 4 \\ [1, 1, (1 - d_K)/4] & \text{for } d_K \equiv 1 \pmod 4, \end{cases}$$

and the inverse of the class containing $[a, b, c]$ is the class containing $[a, -b, c]$ ([2, Theorem 3.9]). We then identify $\mathrm{C}(d_K)$ with the set of all *reduced quadratic forms*, which are characterized by the condition

$$(-a < b \le a < c \text{ or } 0 \le b \le a = c) \quad \text{and} \quad b^2 - 4ac = d_K \tag{4.8}$$

([2, Theorem 2.8]). Note that the above condition for reduced quadratic forms yields

$$a \le \sqrt{-d_K/3} \tag{4.9}$$

([2, p.29]). On the other hand, it is well-known that $\mathrm{C}(d_K)$ is isomorphic to $\mathrm{Gal}(H/K)$ ([2, Theorem 7.7]). And, Stevenhagen ([19]) found an idèle $x_Q \in \mathbb{A}_K^*$ satisfying

$$[x_Q, K]|_H = [a, b, c]$$

as an element of $\mathrm{Gal}(H/K)$ as follows:

Proposition 4.2. *Let $Q = [a, b, c]$ be a reduced quadratic form of discriminant d_K. We define a CM-point*

$$\theta_Q = (-b + \sqrt{d_K})/2a. \tag{4.10}$$

Furthermore, for each prime p we define $x_p \in K_p^*$ as

$$x_p = \begin{cases} a & \text{if } p \nmid a \\ a\theta_Q & \text{if } p \mid a \text{ and } p \nmid c \\ a(\theta_Q - 1) & \text{if } p \mid a \text{ and } p \mid c, \end{cases}$$

and set $x_Q = (x_p)_p \in \mathbb{A}_K^*$. Then the reciprocity map $[x_Q, K]$ satisfies

$$j(\theta_K)^{[x_Q,K]} = j(\theta_K)^{[a,b,c]}.$$

Proof. See [19, §6]. □

The next proposition gives the action of $[x_Q^{-1}, K]$ on K^{ab} by using Shimura's reciprocity law (4.7).

Proposition 4.3. *Let $Q = [a, b, c]$ be a reduced quadratic form of discriminant d_K and θ_Q be as in (4.10). Define $u_Q = (u_p)_p \in \prod_p \mathrm{GL}_2(\mathbb{Z}_p)$ as*

$$u_p = \begin{cases} \begin{pmatrix} a & b/2 \\ 0 & 1 \end{pmatrix} & \text{if } p \nmid a \\ \begin{pmatrix} -b/2 & -c \\ 1 & 0 \end{pmatrix} & \text{if } p \mid a \text{ and } p \nmid c \\ \begin{pmatrix} -a - b/2 & -b/2 - c \\ 1 & -1 \end{pmatrix} & \text{if } p \mid a \text{ and } p \mid c \end{cases} \quad \text{for } d_K \equiv 0 \pmod 4, \tag{4.11}$$

and

$$u_p = \begin{cases} \begin{pmatrix} a & (b-1)/2 \\ 0 & 1 \end{pmatrix} & \text{if } p \nmid a \\ \begin{pmatrix} -(b+1)/2 & -c \\ 1 & 0 \end{pmatrix} & \text{if } p \mid a \text{ and } p \nmid c \\ \begin{pmatrix} -a - (b+1)/2 & (1-b)/2 - c \\ 1 & -1 \end{pmatrix} & \text{if } p \mid a \text{ and } p \mid c \end{cases} \quad \text{for } d_K \equiv 1 \pmod 4. \tag{4.12}$$

If $h \in \mathcal{F}$ is defined and finite at θ_K, then we have

$$h^{u_Q}(\theta_Q) = h(\theta_K)^{[x_Q^{-1},K]}.$$

Proof. See [19, §6]. □

Hence we achieve that for a reduced quadratic form Q of discriminant d_K,

$$j^{u_Q}(\theta_Q)=j(\theta_K)^{[x_Q^{-1},K]}=j(\theta_K)^{[a,-b,c]}.$$

By analyzing the diagram (4.6) and using Shimura's reciprocity law (4.7) Stevenhagen was able to express $\mathrm{Gal}(K_{(N)}/H)$ quite explicitly.

Proposition 4.4. *Let K $(\neq\mathbb{Q}(\sqrt{-1}),\mathbb{Q}(\sqrt{-3}))$ be an imaginary quadratic field and N be a positive integer. Then the group*

$$W_{N,\theta_K}=\left\{\begin{pmatrix}t-B_{\theta_K}s & -C_{\theta_K}s\\ s & t\end{pmatrix}\in\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})\ ;\ t,s\in\mathbb{Z}/N\mathbb{Z}\right\}$$

gives rise to a surjection

$$\begin{array}{rcl}W_{N,\theta_K} & \longrightarrow & \mathrm{Gal}(K_{(N)}/H)\\ \alpha & \longmapsto & (h(\theta_K)\mapsto h^{\alpha}(\theta_K)\ ;\ h\in\mathcal{F}_N \textit{ is defined and finite at } \theta_K)\end{array}$$

with kernel $\{\pm 1_2\}$.

Proof. See [19, §3]. □

Combining all the results we come up with an algorithm to determine the conjugates of the singular value of a modular function.

Theorem 4.5. *Let K $(\neq\mathbb{Q}(\sqrt{-1}),\mathbb{Q}(\sqrt{-3}))$ be an imaginary quadratic field and N be a positive integer. There is a one-to-one correspondence*

$$\begin{array}{rcl}W_{N,\theta_K}/\{\pm 1_2\}\times\mathrm{C}(d_K) & \longrightarrow & \mathrm{Gal}(K_{(N)}/K)\\ (\alpha,Q) & \mapsto & (h(\theta_K)\mapsto h^{\alpha\cdot u_Q}(\theta_Q)\ ;\ h\in\mathcal{F}_N \textit{ is defined and finite at } \theta_K).\end{array}$$

Here, we adopt the notations in Propositions 4.2∼4.4.

Proof. The result follows directly from Propositions 4.2∼4.4. □

Remark 4.6. In particular, the unit element of $W_{N,\theta_K}/\{\pm 1_2\}\times\mathrm{C}(d_K)$ corresponds to the unit element of $\mathrm{Gal}(K_{(N)}/K)$ by the definitions of u_Q and θ_Q. Note that this correspondence, in fact, is not a group homomorphism.

5. Ray class invariants over imaginary quadratic fields

Through out this section let K be an imaginary quadratic field of discriminant d_K, θ_K be as in (4.4) and N (≥ 2) be an integer. We shall prove our main theorem which claims that if $d_K\leq -19$ and $N\geq 3$, then for any nonzero integer m the singular value

$$y_{(0,1/N)}^{4m/\gcd(4,N)}(\theta_K)$$

generates the ray class field $K_{(N)}$ over K.

First, we consider an exceptional case $K=\mathbb{Q}(\sqrt{-3})$ with $\theta_K=(-1+\sqrt{-3})/2$. In the uniformization

$$\begin{array}{rcl}\varphi\ :\ \mathbb{C}/\mathcal{O}_K & \xrightarrow{\sim} & E(\mathbb{C})\ :\ y^2=4x^3-g_2(\theta_K)x-g_3(\theta_K)\\ z & \mapsto & [\wp(z;\mathcal{O}_K):\wp'(z;\mathcal{O}_K):1],\end{array}$$

if we set $z=1/N$, then we have the relation

$$\wp'(1/N;\mathcal{O}_K)^2=4\wp(1/N;\mathcal{O}_K)^3-g_2(\theta_K)\wp(1/N;\mathcal{O}_K)-g_3(\theta_K).$$

Multiplying both sides by $g_3(\theta_K)/\Delta(\theta_K)$ we obtain by (3.12) and (3.13) that

$$\frac{g_3(\theta_K)}{\eta^{12}(\theta_K)}y^2_{(0,1/N)}(\theta_K)=4\frac{g_3(\theta_K)}{\Delta(\theta_K)}\wp(1/N;\mathcal{O}_K)^3-\frac{g_2(\theta_K)g_3(\theta_K)}{\Delta(\theta_K)}\wp(1/N;\mathcal{O}_K)-\frac{g_3(\theta_K)^2}{\Delta(\theta_K)}. \tag{5.1}$$

On the other hand, since $g_2(\theta_K)=0$ ([11, p.37]), we achieve from the definition (3.3) that

$$j(\theta_K)=0,\quad g_3(\theta_K)^2/\Delta(\theta_K)=-1/27\quad\text{and}\quad g_3(\theta_K)/\eta^{12}(\theta_K)=\pm 1/3\sqrt{-3}.$$

Hence the equation (5.1) becomes

$$\pm(1/3\sqrt{-3})y^2_{(0,1/N)}(\theta_K)=4h(\varphi(1/N))+1/27,$$

where h is the Weber function on $E(\mathbb{C})$ defined as in (4.2). Therefore, by Proposition 4.1(i) the singular value

$$y^2_{(0,1/N)}(\theta_K)$$

generates $K_{(N)}$ over K.

Now we investigate the general cases $d_K\leq -19$. We need some lemmas which enable us to compare the absolute values of singular values of certain Siegel functions. For simplicity we let

$$A=|e^{2\pi i\theta_K}|=e^{-\pi\sqrt{-d_K}}\quad\text{and}\quad D=\sqrt{-d_K/3}.$$

Lemma 5.1. *We have the following inequalities:*

(i) *If $d_K\leq -3$, then*

$$1/(1-A^{X/a})<1+A^{X/1.03a} \tag{5.2}$$

for $1\leq a\leq D$ and all $X\geq 1/2$.

(ii) $1+X<e^X$ *for all $X>0$.*

Proof. (i) The inequality (5.2) is equivalent to

$$A^{3X/103a}+A^{X/a}<1.$$

Since $A=e^{-\pi\sqrt{-d_K}}\leq e^{-\pi\sqrt{7}}<1$, $1\leq a\leq D$ and $X\geq 1/2$, we derive

$$A^{3X/103a}+A^{X/a}\leq A^{3/206D}+A^{1/2D}=e^{-3\pi\sqrt{3}/206}+e^{-\pi\sqrt{3}/2}<1$$

by the fact $A^{1/D}=e^{-\pi\sqrt{3}}$. This proves (i).

(ii) Since the function $f(X)=e^X-X-1$ is increasing on $X>0$ and $f(0)=0$, we get (ii). □

Lemma 5.2. *Assume that $d_K\leq -20$ and $N\geq 3$. Let $Q=[a,b,c]$ be a reduced quadratic form of discriminant d_K with θ_Q as in (4.10). If $a\geq 2$, then the inequality*

$$\left|\frac{g_{(2s/N,2t/N)}(\theta_Q)}{g^4_{(s/N,t/N)}(\theta_Q)}\right|<0.996\left|\frac{g_{(0,2/N)}(\theta_K)}{g^4_{(0,1/N)}(\theta_K)}\right|$$

holds for any $(s,t)\in\mathbb{Z}^2-N\mathbb{Z}^2$.

Proof. We may assume that $0\leq s\leq N/2$ and $0\leq t<N$ by Proposition 3.5(i) and (iii). Also note that $2\leq a\leq D$ by (4.9) and $A\leq e^{-\pi\sqrt{20}}<1$. It follows from the infinite product formula (3.10)

that

$$\begin{aligned}
&\left|\left(\frac{g_{(0,2/N)}(\theta_K)}{g^4_{(0,1/N)}(\theta_K)}\right)^{-1}\left(\frac{g_{(2s/N,2t/N)}(\theta_Q)}{g^4_{(s/N,t/N)}(\theta_Q)}\right)\right| \\
\leq\ & A^{1/4+(1/a)(s/N-1/4)}\left|\frac{(1-\zeta_N)^4}{1-\zeta_N^2}\right|\left|\frac{1-e^{2\pi i((2s/N)\theta_Q+2t/N)}}{(1-e^{2\pi i((s/N)\theta_Q+t/N)})^4}\right| \\
&\times\prod_{n=1}^{\infty}\frac{(1+A^n)^8(1+A^{(1/a)(n+2s/N)})(1+A^{(1/a)(n-2s/N)})}{(1-A^n)^2(1-A^{(1/a)(n+s/N)})^4(1-A^{(1/a)(n-s/N)})^4} \\
\leq\ & T(N,s,t)\prod_{n=1}^{\infty}\frac{(1+A^n)^8(1+A^{n/a})(1+A^{(1/a)(n-1)})}{(1-A^n)^2(1-A^{n/a})^4(1-A^{(1/a)(n-1/2)})^4} \quad \text{by the fact } 0\leq s\leq N/2 \\
\leq\ & T(N,s,t)\prod_{n=1}^{\infty}\frac{(1+A^n)^8(1+A^{n/D})(1+A^{(1/D)(n-1)})}{(1-A^n)^2(1-A^{n/D})^4(1-A^{(1/D)(n-1/2)})^4} \quad \text{by the fact } 2\leq a\leq D,
\end{aligned}$$

where

$$T(N,s,t)=A^{1/4+(1/a)(s/N-1/4)}\left|\frac{(1-\zeta_N)^3}{1+\zeta_N}\right|\left|\frac{1+e^{2\pi i((s/N)\theta_Q+t/N)}}{(1-e^{2\pi i((s/N)\theta_Q+t/N)})^3}\right|.$$

If $s=0$, then

$$\begin{aligned}
T(N,s,t) &= A^{1/4-1/4a}\left|\left(\frac{1-\zeta_N}{1-\zeta_N^t}\right)^3\right|\left|\frac{1+\zeta_N^t}{1+\zeta_N}\right| = A^{1/4-1/4a}\left|\left(\frac{\sin(\pi/N)}{\sin(t\pi/N)}\right)^3\right|\left|\frac{\cos(t\pi/N)}{\cos(\pi/N)}\right| \\
&\leq A^{1/8} \quad \text{by the fact } 2\leq a\leq D \\
&\leq e^{-\pi\sqrt{20}/8}<0.173 \quad \text{by the fact } d_K\leq -20.
\end{aligned}$$

If $s\neq 0$, then

$$\begin{aligned}
T(N,s,t) &\leq A^{1/4+(1/a)(1/N-1/4)}\left|\frac{(1-\zeta_N)^3}{1+\zeta_N}\right|\frac{1+A^{1/Na}}{(1-A^{1/Na})^3} \quad \text{by the fact } 1\leq s\leq N/2 \\
&\leq A^{1/4+(1/2)(1/N-1/4)}\left|\frac{(1-\zeta_N)^3}{1+\zeta_N}\right|\frac{1+A^{1/ND}}{(1-A^{1/ND})^3} \quad \text{by the fact } 2\leq a\leq D \\
&= e^{-\pi\sqrt{20}(1/8+1/2N)}\frac{4\sin^3(\pi/N)}{\cos(\pi/N)}\frac{1+e^{-\pi\sqrt{3}/N}}{(1-e^{-\pi\sqrt{3}/N})^3} \quad \text{by the facts } d_K\leq -20 \text{ and } A^{1/D}=e^{-\pi\sqrt{3}} \\
&< 0.267 \quad \text{from the graph for } N\geq 3 \text{ (Figure 1).}
\end{aligned}$$

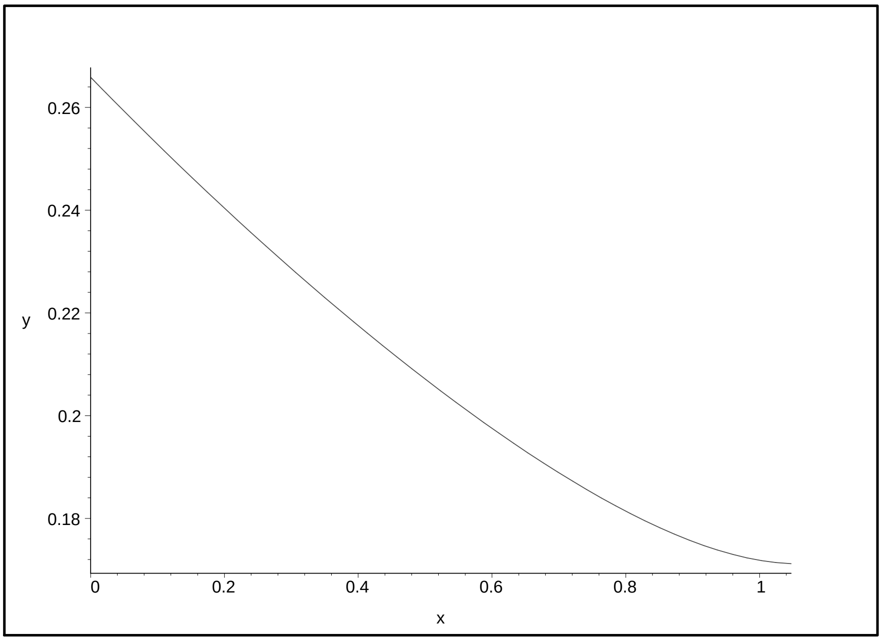

FIGURE 1. $Y = e^{-\pi\sqrt{20}(1/8+X/2\pi)}\frac{4\sin^3 X}{\cos X}\frac{1+e^{-\sqrt{3}X}}{(1-e^{-\sqrt{3}X})^3}$ for $0 < X \leq \pi/3$

Therefore, we derive that

$$\begin{aligned}
&\left|\left(\frac{g_{(0,2/N)}(\theta_K)}{g^4_{(0,1/N)}(\theta_K)}\right)^{-1}\left(\frac{g_{(2s/N,2t/N)}(\theta_Q)}{g^4_{(s/N,t/N)}(\theta_Q)}\right)\right| \\
<\ & 0.267\prod_{n=1}^{\infty}\frac{(1+A^n)^8(1+A^{n/D})(1+A^{(1/D)(n-1)})}{(1+A^{n/1.03})^{-2}(1+A^{n/1.03D})^{-4}(1+A^{(1/1.03D)(n-1/2)})^{-4}} \quad \text{by Lemma 5.1(i)} \\
<\ & 0.267\prod_{n=1}^{\infty}e^{8A^n+A^{n/D}+A^{(1/D)(n-1)}+2A^{n/1.03}+4A^{n/1.03D}+4A^{(1/1.03D)(n-1/2)}} \quad \text{by Lemma 5.1(ii)} \\
=\ & 0.267e^{8A/(1-A)+(A^{1/D}+1)/(1-A^{1/D})+2A^{1/1.03}/(1-A^{1/1.03})+(4A^{1/1.03D}+4A^{1/2.06D})/(1-A^{1/1.03D})} \\
\leq\ & 0.267e^{8e^{-\pi\sqrt{20}}/(1-e^{-\pi\sqrt{20}})+(e^{-\pi\sqrt{3}}+1)/(1-e^{-\pi\sqrt{3}})+2e^{-\pi\sqrt{20}/1.03}/(1-e^{-\pi\sqrt{20}/1.03})} \\
& \times e^{(4e^{-\pi\sqrt{3}/1.03}+4e^{-\pi\sqrt{3}/2.06})/(1-e^{-\pi\sqrt{3}/1.03})} \quad \text{by the facts } A \leq e^{-\pi\sqrt{20}} \text{ and } A^{1/D} = e^{-\pi\sqrt{3}} \\
<\ & 0.996.
\end{aligned}$$

This proves the lemma. □

Lemma 5.3. *Assume that $d_K \leq -11$ and $N \geq 3$. Then the inequality*

$$\left|\frac{g_{(2s/N,2t/N)}(\theta_K)}{g^4_{(s/N,t/N)}(\theta_K)}\right| < 0.614\left|\frac{g_{(0,2/N)}(\theta_K)}{g^4_{(0,1/N)}(\theta_K)}\right|$$

holds for any $(s,t) \in \mathbb{Z}^2 - N\mathbb{Z}^2$ such that $(s,t) \not\equiv (0,\pm 1) \pmod N$.

Proof. We may also assume that $0 \le s \le N/2$ and $0 \le t < N$ by Proposition 3.5(i) and (iii). From the infinite product formula (3.10) we establish that

$$\begin{aligned}
&\left| \left(\frac{g_{(0,2/N)}(\theta_K)}{g^4_{(0,1/N)}(\theta_K)} \right)^{-1} \left(\frac{g_{(2s/N,2t/N)}(\theta_K)}{g^4_{(s/N,t/N)}(\theta_K)} \right) \right| \\
\le\ & A^{s/N} \left| \frac{(1-\zeta_N)^4}{1-\zeta_N^2} \right| \left| \frac{1-e^{2\pi i((2s/N)\theta_K+2t/N)}}{(1-e^{2\pi i((s/N)\theta_K+t/N)})^4} \right| \prod_{n=1}^{\infty} \frac{(1+A^n)^8(1+A^{n+2s/N})(1+A^{n-2s/N})}{(1-A^n)^2(1-A^{n+s/N})^4(1-A^{n-s/N})^4} \\
\le\ & T(N,s,t) \prod_{n=1}^{\infty} \frac{(1+A^n)^9(1+A^{n-1})}{(1-A^n)^6(1-A^{n-1/2})^4} \quad \text{by the fact } 0 \le s \le N/2,
\end{aligned}$$

where

$$T(N,s,t) = A^{s/N} \left| \frac{(1-\zeta_N)^3}{1+\zeta_N} \right| \left| \frac{1+e^{2\pi i((s/N)\theta_K+t/N)}}{(1-e^{2\pi i((s/N)\theta_K+t/N)})^3} \right|.$$

If $s = 0$, then $N \ge 4$ and $2 \le t \le N-2$ by the assumption $(s,t) \not\equiv (0, \pm 1) \pmod N$; hence

$$\begin{aligned}
T(N,s,t) &= \left| \left(\frac{1-\zeta_N}{1-\zeta_N^t} \right)^3 \right| \left| \frac{1+\zeta_N^t}{1+\zeta_N} \right| = \left| \left(\frac{\sin(\pi/N)}{\sin(t\pi/N)} \right)^3 \right| \left| \frac{\cos(t\pi/N)}{\cos(\pi/N)} \right| \\
&\le \left(\frac{\sin(\pi/N)}{\sin(2\pi/N)} \right)^3 \frac{\cos(2\pi/N)}{\cos(\pi/N)} = \frac{2\cos^2(\pi/N)-1}{8\cos^4(\pi/N)} \\
&< 0.125 \quad \text{from the graph for } N \ge 4 \text{ (Figure 2).}
\end{aligned}$$

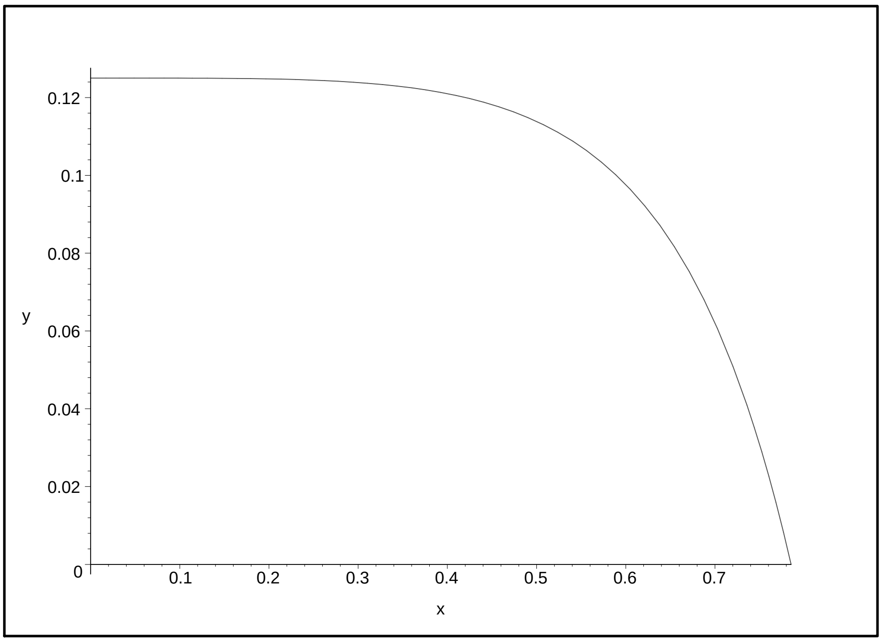

FIGURE 2. $Y = \frac{2\cos^2 X - 1}{8\cos^4 X}$ for $0 < X \le \pi/4$

If $s \neq 0$, then

$$\begin{aligned}
T(N,s,t) &\leq A^{1/N}\left|\frac{(1-\zeta_N)^3}{1+\zeta_N}\right|\frac{1+A^{1/N}}{(1-A^{1/N})^3} = \frac{4\sin^3(\pi/N)}{\cos(\pi/N)}\frac{A^{1/N}(1+A^{1/N})}{(1-A^{1/N})^3}\\
&\leq \frac{4\sin^3(\pi/N)}{\cos(\pi/N)}\frac{e^{-\pi\sqrt{11}/N}(1+e^{-\pi\sqrt{11}/N})}{(1-e^{-\pi\sqrt{11}/N})^3} \quad \text{by the fact } d_K \leq -11\\
&< 0.22 \quad \text{from the graph for } N \geq 3 \text{ (Figure 3).}
\end{aligned}$$

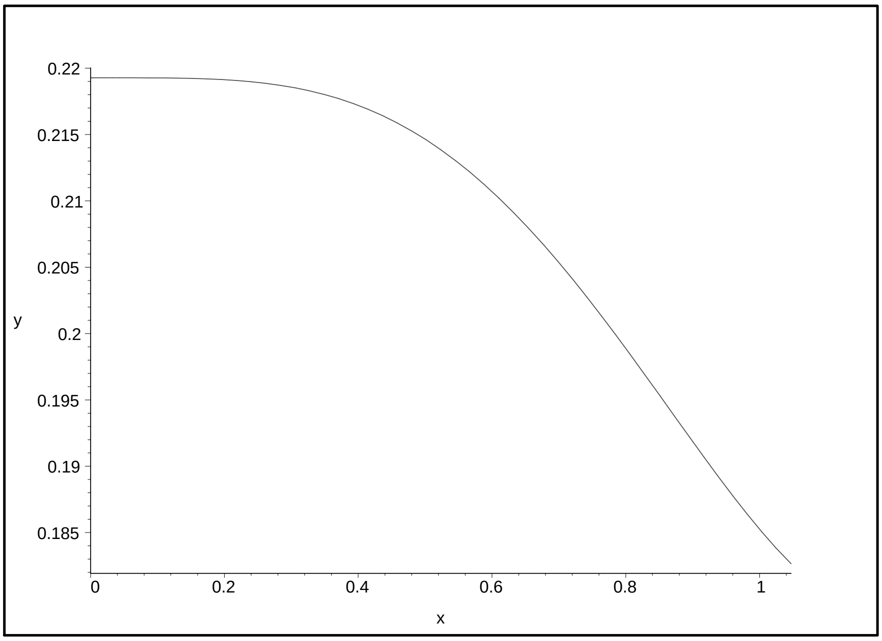

FIGURE 3. $Y = \frac{4\sin^3 X}{\cos X}\frac{e^{-\sqrt{11}X}(1+e^{-\sqrt{11}X})}{(1-e^{-\sqrt{11}X})^3}$ for $0 < X \leq \frac{\pi}{3}$

Therefore, we get that

$$\begin{aligned}
&\left|\left(\frac{g_{(0,2/N)}(\theta_K)}{g^4_{(0,1/N)}(\theta_K)}\right)^{-1}\left(\frac{g_{(2s/N,2t/N)}(\theta_K)}{g^4_{(s/N,t/N)}(\theta_K)}\right)\right|\\
&< 0.22\prod_{n=1}^{\infty}\frac{(1+A^n)^9(1+A^{n-1})}{(1+A^{n/1.03})^{-6}(1+A^{(1/1.03)(n-1/2)})^{-4}} \quad \text{by Lemma 5.1(i)}\\
&< 0.22\prod_{n=1}^{\infty}e^{9A^n+A^{n-1}+6A^{n/1.03}+4A^{(1/1.03)(n-1/2)}} \quad \text{by Lemma 5.1(ii)}\\
&= 0.22e^{(9A+1)/(1-A)+(6A^{1/1.03}+4A^{1/2.06})/(1-A^{1/1.03})}\\
&\leq 0.22e^{(9e^{-\pi\sqrt{11}}+1)/(1-e^{-\pi\sqrt{11}})+(6e^{-\pi\sqrt{11}/1.03}+4e^{-\pi\sqrt{11}/2.06})/(1-e^{-\pi\sqrt{11}/1.03})} \quad \text{by the facts } A \leq e^{-\pi\sqrt{11}}\\
&< 0.614.
\end{aligned}$$

This proves the lemma. $\square$

Theorem 5.4. *Let K be an imaginary quadratic field of discriminant d_K (≤ -19), θ_K be as in (4.4) and N (≥ 3) be an integer. Then for any nonzero integer m, the singular value*

$$y_{(0,1/N)}^{4m/\gcd(4,N)}(\theta_K)$$

generates the ray class field $K_{(N)}$ over K.

Proof. For simplicity we put $y(\tau)=y_{(0,1/N)}^{4m/\gcd(4,N)}(\tau)$. Since $y(\tau)$ belongs to $\mathcal{F}_N$ by Lemma 3.9, its singular value $y(\theta_K)$ lies in $K_{(N)}$ by Proposition 4.1(ii). Hence, if we show that the only element of $\mathrm{Gal}(K_{(N)}/K)$ leaving the value $y(\theta_K)$ fixed is the unit element, then we can conclude that $y(\theta_K)$ generates $K_{(N)}$ over K by Galois theory.

Any conjugate of $y(\theta_K)$ is of the form

$$y^{\alpha\cdot u_Q}(\theta_Q)$$

for some $\alpha=\begin{pmatrix} t-B_{\theta_K}s & -C_{\theta_K}s \\ s & t\end{pmatrix}\in W_{N,\theta_K}$ and a reduced quadratic form $Q=[a,b,c]$ of discriminant d_K by Theorem 4.5. Assume that $y(\theta_K)=y^{\alpha\cdot u_Q}(\theta_Q)$. If $d_K=-19$, then $h_K=1$ ([2, Theorem 12.34]), so $a=1$. If $d_K\leq -20$, then Lemma 5.2 leads us to take $a=1$. And, we derive from the condition (4.8) for reduced quadratic forms that

$$Q=[a,b,c]=\begin{cases}[1,0,-d_K/4] & \text{for } d_K\equiv 0 \pmod 4\\ [1,1,(1-d_K)/4] & \text{for } d_K\equiv 1 \pmod 4,\end{cases}$$

which represents the unit element of $\mathrm{C}(d_K)$. It follows that $\theta_Q=\theta_K$ and

$$u_Q=\begin{cases}\begin{pmatrix}1 & b/2\\ 0 & 1\end{pmatrix} & \text{for } d_K\equiv 0 \pmod 4\\[2ex] \begin{pmatrix}1 & (b-1)/2\\ 0 & 1\end{pmatrix} & \text{for } d_K\equiv 1 \pmod 4\end{cases}$$

as an element of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ by the definitions (4.11) and (4.12). Thus we deduce from Proposition 3.8 that

$$\begin{aligned} y(\theta_K)=y^{\alpha\cdot u_Q}(\theta_Q) &\doteq \left(\frac{g_{(0,2/N)\alpha u_Q}(\theta_Q)}{g^4_{(0,1/N)\alpha u_Q}(\theta_Q)}\right)^{4m/\gcd(4,N)}\\ &\doteq \begin{cases}\left(\dfrac{g_{(2s/N,(2s/N)(b/2)+2t/N)}(\theta_K)}{g^4_{(s/N,(s/N)(b/2)+t/N)}(\theta_K)}\right)^{4m/\gcd(4,N)} & \text{for } d_K\equiv 0 \pmod 4\\[3ex] \left(\dfrac{g_{(2s/N,(2s/N)(b-1)/2+2t/N)}(\theta_K)}{g^4_{(s/N,(s/N)(b-1)/2+t/N)}(\theta_K)}\right)^{4m/\gcd(4,N)} & \text{for } d_K\equiv 1 \pmod 4,\end{cases}\end{aligned}$$

where $\doteq$ stands for the equality up to a root of unity. Now we get $(s,t)\equiv(0,\pm1) \pmod N$ by Lemma 5.3, which shows that α is the unit element of $W_{N,\theta_K}/\{\pm 1_2\}$. Hence $(\alpha,Q)\in W_{N,\theta_K}/\{\pm 1_2\}\times \mathrm{C}(d_K)$ represents the unit element of $\mathrm{Gal}(K_{(N)}/K)$ by Remark 4.6. Therefore, $y(\theta_K)$ indeed generates $K_{(N)}$ over K. □

Corollary 5.5. *Let K be an imaginary quadratic field of discriminant d_K (≤ -19), θ_K be as in (4.4) and N (≥ 3) be an odd integer. Then for any nonzero integer m, the singular value*

$$g_{(0,1/N)}^{12Nm/\gcd(6,N)}(\theta_K)$$

generates $K_{(N)}$ over K.

Proof. Let $g(\tau)=g_{(0,1/N)}^{12Nm/\gcd(6,N)}(\tau)$. Since $g(\tau)\in\mathcal{F}_N$ by Proposition 3.8, its singular value $g(\theta_K)$ lies in $K_{(N)}$ by Proposition 4.1(ii). On the other hand, since $K(g(\theta_K))$ is an abelian extension of K as a subfield of $K_{(N)}$, it contains all conjugates of $g(\theta_K)$. Now that we are assuming N (≥ 3) is odd, $\left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right)\in\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ belongs to W_{N,θ_K} and satisfies

$$g(\theta_K)^{\left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right)}=g_{(0,1/N)\left(\begin{smallmatrix}2&0\\0&2\end{smallmatrix}\right)}^{12Nm/\gcd(6,N)}(\theta_K)=g_{(0,2/N)}^{12Nm/\gcd(6,N)}(\theta_K)$$

by Proposition 3.8. Thus $K(g(\theta_K))$ contains the singular value

$$\left(\frac{g_{(0,2/N)}(\theta_K)}{g_{(0,1/N)}^4(\theta_K)}\right)^{12Nm/\gcd(6,N)}=\left(y_{(0,1/N)}^{4m/\gcd(4,N)}(\theta_K)\right)^{3N\gcd(4,N)/\gcd(6,N)},$$

which implies that $K(g(\theta_K))$ is all of $K_{(N)}$ by Theorem 5.4. $\square$

Lemma 5.6. *If $z\in\mathfrak{H}$ is imaginary quadratic, then the singular value $j(z)$ is a real algebraic integer.*

Proof. See [11, Chapter 5 Theorem 4]. $\square$

Proposition 5.7. *Let K be an imaginary quadratic field, θ_K be as in (4.4) and N (≥ 3) be an integer. Then the singular values*

$$g_{(0,1/N)}^{12N/\gcd(6,N)}(\theta_K)\quad\text{and}\quad\begin{cases}y_{(0,1/N)}^{12N/\gcd(6,N)}(\theta_K) & \text{if } N \text{ has at least two prime factors in } \mathbb{Z}\\ N^{48N/\gcd(6,N)}y_{(0,1/N)}^{12N/\gcd(6,N)}(\theta_K) & \text{if } N \text{ is a prime power}\end{cases}$$

are real algebraic integers. Hence their minimal polynomials over K have integer coefficients.

Proof. Let $g(\tau)=g_{(0,1/N)}^{12N/\gcd(6,N)}(\tau)$ and

$$h(\tau)=\begin{cases}y_{(0,1/N)}^{12N/\gcd(6,N)}(\tau) & \text{if } N \text{ has at least two prime factors in } \mathbb{Z}\\ N^{48N/\gcd(6,N)}y_{(0,1/N)}^{12N/\gcd(6,N)}(\tau) & \text{if } N \text{ is a prime power.}\end{cases}$$

Then $g(\tau)$ and $h(\tau)$ are integral over $\mathbb{Z}[j(\tau)]$ by Proposition 3.7; and hence their singular values $g(\theta_K)$ and $h(\theta_K)$ are algebraic integers by Lemma 5.6. On the other hand, the infinite product formula (3.10) yields

$$g(\theta_K)=q_{\theta_K}^{N/\gcd(6,N)}(2\sin(2\pi/N))^{12N/\gcd(6,N)}\prod_{n=1}^{\infty}(1-2\cos(4\pi/N)q_{\theta_K}^n+q_{\theta_K}^{2n})^{12N/\gcd(6,N)},$$

and

$$y^{12N/\gcd(6,N)}(\theta_K)=\frac{q_{\theta_K}^{N/\gcd(6,N)}(2\sin(2\pi/N))^{12N/\gcd(6,N)}\prod_{n=1}^{\infty}(1-2\cos(4\pi/N)q_{\theta_K}^n+q_{\theta_K}^{2n})^{12N/\gcd(6,N)}}{q_{\theta_K}^{4N/\gcd(6,N)}(2\sin(\pi/N))^{48N/\gcd(6,N)}\prod_{n=1}^{\infty}(1-2\cos(2\pi/N)q_{\theta_K}^n+q_{\theta_K}^{2n})^{48N/\gcd(6,N)}},$$

where

$$q_{\theta_K}=e^{2\pi i\theta_K}=\begin{cases}e^{-\pi\sqrt{-d_K}} & \text{for } d_K\equiv 0 \pmod 4\\ -e^{-\pi\sqrt{-d_K}} & \text{for } d_K\equiv 1 \pmod 4).\end{cases}$$

Therefore $g(\theta_K)$ and $h(\theta_K)$ are real numbers. If we set $x=g(\theta_K)$ or $h(\theta_K)$, then

$$[\mathbb{Q}(x):\mathbb{Q}]=\frac{[K(x):K]\cdot[K:\mathbb{Q}]}{[K(x):\mathbb{Q}(x)]}=\frac{[K(x):K]\cdot 2}{2}=[K(x):K],$$

which implies that the coefficients of the minimal polynomial of x over K are integers. $\square$

Example 5.8. Let $K = \mathbb{Q}(\sqrt{-10})$, then $d_K = -40$ and $\theta_K = \sqrt{-10}$. The reduced quadratic forms of discriminant d_K are

$$Q_1 = [1, 0, 10] \quad \text{and} \quad Q_2 = [2, 0, 5],$$

so we get

$$\theta_{Q_1} = \sqrt{-10},\ u_{Q_1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \theta_{Q_2} = \sqrt{-10}/2,\ u_{Q_2} = \begin{pmatrix} 2 & -3 \\ 3 & 4 \end{pmatrix}.$$

Furthermore, if $N = 6$, then

$$W_{6,\theta_K}/\{\pm 1_2\} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ 5 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix} \right\}.$$

By Theorem 5.4 the singular value $y^{12}_{(0,1/6)}(\theta_K)$ generates $K_{(6)}$ over K, and its minimal polynomial is as follows:

$$\begin{aligned}
&\min(y^{12}_{(0,1/6)}(\theta_K), K) \\
= &\prod_{r=1}^{2} \prod_{\alpha \in W_{6,\theta_K}/\{\pm 1_2\}} \left(X - \left(\frac{g^{12}_{(0,2/6)}(\tau)}{g^{48}_{(0,1/6)}(\tau)} \right)^{\alpha u_{Q_r}} (\theta_{Q_r}) \right) = \prod_{r=1}^{2} \prod_{\alpha \in W_{6,\theta_K}/\{\pm 1_2\}} \left(X - \frac{g^{12}_{(0,2/6)\alpha U_{Q_r}}(\theta_{Q_r})}{g^{48}_{(0,1/6)\alpha U_{Q_r}}(\theta_{Q_r})} \right) \\
= &X^{16} - 56227499765918216689444911216X^{15} \\
&+28198738767573877103982180845427211416X^{14} \\
&-61006294392822456973543787353433426528859172752X^{13} \\
&+24191545040559618198685578078066621024919984909895925564X^{12} \\
&-1457219992512158403396945180026448081831307850098282381377715440X^{11} \\
&-1875247086634588418900161009847749757705491090331618598955145878499352X^{10} \\
&-3204258054536691403559566745682638856959186166279206475927474345038453779344X^{9} \\
&+383798110212800409840846851392850879043779134397546083788605170327010622235878X^{8} \\
&-115423974200159134410244151892157361168179592425853550820710288184072396692478416X^{7} \\
&+334107284582565793933974554285013907697215168114012280251572770023994260474295208X^{6} \\
&-2413062017539132381926952150397596657649211631905734942002508919329018160X^{5} \\
&+5947186157319106561144943221021199418610488121986658654341036924X^{4} \\
&-5317595247800083950930014176690955051475061944750295248X^{3} \\
&+797299465586120177639706616225451835994220376X^{2} \\
&-29812156397602328057777202393119664X + 282429536481.
\end{aligned}$$

6. Application to normal bases

Let L be a finite abelian extension of a number field K with $G = \mathrm{Gal}(L/K) = \{\gamma_1 = \mathrm{Id}, \cdots, \gamma_n\}$. From the normal basis theorem ([21, §8.11]) we know that there exists a normal basis of L over K, namely, a K-basis of the form $\{x^\gamma ; \gamma \in G\}$ for a single element $x \in L$. Hence L is understood as a free $K[G]$-module of rank 1.

Okada ([13]) showed that if k (≥ 1) and q (≥ 3) are integers with k odd and T is a set of representatives for which $(\mathbb{Z}/q\mathbb{Z})^\times = T \cup (-T)$, then the real numbers $(1/\pi)^k (d/dz)^k (\cot \pi z)|_{z=a/q}$ for $a \in T$ form a normal basis of the maximal real subfield of $\mathbb{Q}(e^{2\pi i/q})$ over $\mathbb{Q}$. Replacing the cotangent function by the Weierstrass $\wp$-function with fundamental period i and 1, he further

obtained in [14] normal bases of class fields over the Gauss field $\mathbb{Q}(\sqrt{-1})$. This result was due to the fact that the Gauss field has class number one, which can be naturally extended to any imaginary quadratic field of class number one.

After Okada, Taylor ([20]) and Schertz ([16]) established Galois module structures of rings of integers of certain abelian extensions over an imaginary quadratic field, which are analogues to the cyclotomic case ([12]). They also found normal bases by special values of modular functions. And, Komatsu ([8]) considered certain abelian extensions L and K of $\mathbb{Q}(e^{2\pi i/5})$ and constructed a normal basis of L over K by special values of Siegel modular functions.

In this short section we shall construct normal bases of ray class fields over imaginary quadratic fields by means of the singular values of y-coordinates of certain elliptic curve with complex multiplication as in the beginning of §5.

Lemma 6.1. *Let L be a finite Galois extension of a number field K with $\mathrm{Gal}(L/K) = \{\gamma_1 = \mathrm{Id}, \cdots, \gamma_n\}$. Assume that there exists an element $x \in L$ such that*

$$|x^{\gamma_m}/x| < 1 \quad \text{for } 1 < m \leq n.$$

Take a suitably large positive integer s such that

$$|x^{\gamma_m}/x|^s \leq 1/n \quad \text{for } 1 < m \leq n.$$

Then the conjugates of x^s form a normal basis of L over K.

Proof. See [7, Theorem Theorem 2.4]. □

Theorem 6.2. *Let K be an imaginary quadratic field of discriminant d_K (≤ -19), θ_K be as in (4.4) and N (≥ 3) be an integer. If s is any positive integer such that*

$$s \geq (\gcd(4, N)/4) \log_{1/0.996}[K_{(N)} : K],$$

then the conjugates of the singular value

$$y_{(0,1/N)}^{4s/\gcd(4,N)}(\theta_K)$$

form a normal basis of $K_{(N)}$ over K.

Proof. Let

$$x = y_{(0,1/N)}^{4/\gcd(4,N)}(\theta_K).$$

In the proof of Theorem 5.4 we have proved that if $\sigma \in \mathrm{Gal}(K_{(N)}/K)$ is not the unit element, then

$$|x^\sigma/x| < 0.996^{4/\gcd(4,N)}$$

by virtue of Lemmas 5.2 and 5.3. Hence Lemma 6.1 proves the assertion. □

References

1. B. Cho and J. K. Koo, *Constructions of ray class fields over imaginary quadratic fields and applications*, Q. J. Math. 61 (2010), 199–216.
2. D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, Class Field, and Complex Multiplication*, A Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, 1989.
3. F. Diamond and J. Shurman, *A First Course in Modular Forms*, Grad. Texts in Math. 228, Springer-Verlag, New York, 2005.
4. G. Gras, *Class Field Theory*, Springer Monographs in Math., Springer-Verlag, Berlin, 2003.
5. B. Gross and D. Zagier, *On singular moduli*, J. reine angew. Math. 355 (1985), 191–220.
6. H. Hasse, *Neue Begründung der komplexen Multiplikation. I*, J. Reine Angew. Math. 157 (1927), 115–139.
7. H. Y. Jung, J. K. Koo and D. H. Shin, *Normal bases of ray class fields over imaginary quadratic fields*, http://arxiv.org/abs/1007.2312, to appear in Math. Zeit.

8. K. Komatsu, *Construction of a normal basis by special values of Siegel modular functions*, Proc. Amer. Math. Soc. 128 (2000), no. 2, 315–323.
9. J. K. Koo and D. H. Shin, *On some arithmetic properties of Siegel functions*, Math. Zeit. 264 (2010) 137–177.
10. D. Kubert and S. Lang, *Modular Units*, Grundlehren der mathematischen Wissenschaften 244, Spinger-Verlag, New York-Berlin, 1981.
11. S. Lang, *Elliptic Functions*, With an appendix by J. Tate, 2nd edition, Grad. Texts in Math. 112, Springer-Verlag, New York, 1987.
12. H. W. Leopoldt, *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, J. Reine Angew. Math. 201 (1959) 119–149.
13. T. Okada, *On an extension of a theorem of S. Chowla*, Acta Arith. 38 (1980/81), no. 4, 341–345.
14. T. Okada, *Normal bases of class field over Gauss' number field*, J. London Math. Soc. (2) 22 (1980), no. 2, 221–225.
15. K. Ramachandra, *Some applications of Kronecker's limit formula*, Ann. of Math. (2) 80 (1964), 104–148.
16. R. Schertz, *Galoismodulstruktur und elliptische Funktionen*, J. Number Theory 39 (1991), no. 3, 285–326.
17. G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton University Press, Princeton, N. J., 1971.
18. J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer-Verlag, New York, 1992.
19. P. Stevenhagen, *Hilbert's 12th problem, complex multiplication and Shimura reciprocity*, Class Field Theory-Its Centenary and Prospect (Tokyo, 1998), 161–176, Adv. Stud. Pure Math. 30, Math. Soc. Japan, Tokyo, 2001.
20. M. J. Talyor, *Relative Galois module structure of rings of integers and elliptic functions II*, Ann. of Math. (2) 121 (1985), no. 3, 519–535.
21. B. L. van der Waerden, *Algebra, Vol I*, Springer-Verlag, New York, 1991.

Department of Mathematical Sciences, KAIST
Current address: Daejeon 373-1, Korea
E-mail address: jkkoo@math.kaist.ac.kr

Department of Mathematical Sciences, KAIST
Current address: Daejeon 373-1, Korea
E-mail address: shakur01@kaist.ac.kr